NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program Peer Review 2006 Inter-Control Center Communications Protocol Assessment

John Michalski, Principal Investigator

Sandia National Laboratories

(505) 844-3122

jtmicha@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Work Package Description

- **ICCP Task 1**

Task performed by: SNL

  - **Investigate the secure ICCP protocol**
    Investigate the integration and implementation issues associated with the introduction of the secure ICCP protocol into the Electrical Utility Industry.

Provide answers to the following questions:

1. What are some of the network configuration issues that need to be identified when deploying secure ICCP? (Certificate Based PKI)
2. What are the transition issues that need to be addressed when moving from a non-secure to a secure form of ICCP? Any alternatives?
3. What are the performance issues surrounding the new secure implementation?
4. What role does Quality of Service play when deploying secure ICCP?
5. What are some of the vulnerabilities that remain “after” the deployment of secure ICCP?

Total FY 06 Task Budget 344k

Goal: Providing a Secure Data Exchange Environment

Work Package Description

- **ICCP Task 2** **Task performed by: INL & PNNL**

  – **Identify ICCP protocol vulnerabilities**
  Investigate typical ICCP applications to identify vulnerabilities that might be exploited to either corrupt critical data or to use as an entry point into the SCADA/EMS

1. Design and build a “fuzzer” device to identify vulnerabilities associated with some implementations of ICCP. (SISCO, LiveData)
2. Build exploits associated with discovered vulnerabilities
3. Push exploits out against a ICCP configured Intrusion Detection device to determine the value of protection
4. Identify new exploit signature profiles to protect ICCP integrated networks
5. Work with Vendors to patch exploitable vulnerabilities

Total FY 06 Task Budget 300k

Goal: Providing a Secure Data Exchange Environment

Industry Needs

The ICCP Work Package addresses Industry needs specifically in the electrical Utility industry where the authenticated exchange of power data is critical to the coordination and distribution of electrical power.

- Energy Stakeholders need:
  - Guidance in the implementation and adaptation of a PKI architecture to provide authentication and confidentiality for ICCP data transport.
  - A “systems view” for providing a secure end-to-end communication path.
- Product Developers Need:
  - The identification of new vulnerabilities that can impact the ICCP data exchange environment.
  - Guidance in identifying the appropriate technology insertion to protect the Electronic Security Perimeter.

Industry Benefits (Impacts)

Benefits of ICCP Work Package:

- Provide "**Best Practice**" implementation of PKI Certificate Architecture to enhance the protection of ICCP data exchanges
- Provide a secure architecture based on a ***system view*** of Operational, Configuration and Performance issues associated with the introduction of secure ICCP
- Identify **new vulnerabilities** between ICCP Client and Server configurations and develop mitigation techniques
- **Report the effectiveness** of existing ICCP-specific security technologies to detect newly discovered vulnerabilities

Technical Approach

- **ICCP Task 1**
  - **Investigate the secure ICCP protocol**
  - Gather information on how a Utility communication architecture is setup and utilized. (Representative structure = Western InterConnection)
  - Use in-house expertise to provide knowledge and guidance in the implementation and integration of a PKI structure onto the architecture
  - Establish a representative Client/Server ICCP structure to benchmark and measure performance attributes associated with the different allowable secure ICCP configurations.
  - Utilize SNL's communication modeling capability to create scenarios of Wide Area Network architectures to measure the impact of Quality-of-Service (QoS) on ICCP data streams
  - Analyze communication path based on elements of Information Assurance (IA) to identify which elements are not addressed by proposed solution and provide mitigation

Technical Approach (cont)

- **ICCP Task 2**
  - **Identify ICCP protocol vulnerabilities:**

1. Develop an ICCP assessment tool a “fuzzer” to evaluate vendor ICCP communication stacks.
2. Write a plan to use the tool developed to evaluate the SISCO and LiveDate ICCP communication stacks (Identify vulnerabilities)
3. Create exploits, execute assessments. Evaluate the effectiveness of existing ICCP-specific security technologies.
4. Work with vendors to mitigate exploitable vulnerabilities
5. Report Findings

Collaborations and Partnerships

David R. Ambrose.

SCADA System Manager. Western Area Power Administration

Chair, Western Electricity Coordinating Council

- Requested support on the Introduction of secure ICCP into the Western Interconnection.
  - NSTB provided initial report on the integration issues associated with secure ICCP and the Public Key Infrastructure
  - NSTB provided a Slide briefing form Mr. Ambrose
    - Briefed at the Date Exchange Working Group (DEWG) hosted by the Western Electric Coordinating Council (WECC)
    - Briefed at the DEWG hosted by North American Electricity Reliability Council

Herb Falk.

SISCO Inc. Product SME, Member of the International Electro technical Commission (IEC) Technical Committee 57 Working Group 15 (ICCP-IEC60870-6-TASE.2).

- (Needs more voices interested in pushing standards that improve security)

Michael Zola

LiveDate Inc. Product SME,

- (Interested in fuzzer output, product improvement)

Technical Progress - Accomplishments

- Task 1
  - Complete initial certificate server and CRL implementation analysis. Provided interim report and slide presentation.
  - Completed a test plan based on the configurations and interactions needed to support the secure ICCP performance research.

  Task 2
  - Developed preliminary version of “fuzzer” which will be used to assess the ICCP protocol stacks.
  - Completed Draft implementation plan to use the tool to evaluate systems from different vendors (SISCO and LiveData)

Backup Slides

Back-up Slide Roadmap

Roadmap to Secure Control Systems in the Energy Sector

- Section 4:16 Control System Security Goals
- Roadmap Goal #1 Measure and assess security posture
- Challenges:
  - The ability to determine the impact of adding security to an installed control system base.
- Milestones:
  - 2008: 50% of asset owners and operators create or review implementation plans with respect to the insertion of secure ICCP.
- Selected Priority: Security Tools and Practices
  - Perform self assessment of control systems
  - Analyze risk based on implementation, identify residual risk.
- Roadmap Goal #2 Develop and integrate protective measures
- Challenges:
  - No security technology that is added to aid the protection of a network, process, or device is inserted without some measurable form of hindrance or degradation.
- Milestones
  - 2009: 50% of network administrators identify the best means of protecting the transit of ICCP database traffic
- Selected Priority:
  - Provide alternatives to proposed integrated security
  - Provide mitigation for residual risk
  - Make available and disseminate best practices for control system security
- Section 4:18 Control System Security
- Roadmap Process and technology improvement cycles
- Identify and understand security risks
- Implement security tools and practices

Back-up Slide Blog Discussions

- **Website to exchange information between SCADA engineers**

"-----Original Message-----
From: scada-bounces@lists.iinet.net.au
To: scada@lists.iinet.net.au
Sent: Mon Dec 12 09:01:18 2005
Subject: [SCADA] Re: Secure ICCP (IEC 60870-6 TASE.2) Question

> I understand that most of the North American based data exchange
> working groups have secure ICCP implementations planned for 2007/2008
> as part of increasing security around the NEC CIP (NERC 1300)
> standards. Some discussion with the telecommunications working groups
> seem to indicate that they will also be encrypting the ICCP WAN
> networks (VPN/IP50) to also support NERC CIP.
>
> I had always thought that one would select either secure ICCP (session
> layer encryption) OR VPN/IP (network level encryption). I didn't see
> any benefit to the double encryption. Am I missing something here?